CLAIMS

1. A packet routing device for routing packet data to be transmitted between a first terminal device on an external network and a second terminal device on a home network, comprising:

a reception unit operable to receive the packet data complying with one of a plurality of secure protocols from the first terminal device via the external network;

a judgment unit operable to judge types of secure protocols, encryption algorithms and encryption keys used for communications via the external network and communications via the home network;

a conversion unit operable to convert the secure protocol for the packet data received by the reception unit into a second secure protocol for the home network, based on the judgment made by the judgment unit; and

an outputting unit operable to output, to the second terminal device, the packet data whose protocol has been converted by the conversion unit.

2. The packet routing device according to Claim 1, further comprising:

a source acquisition unit operable to acquire address information of the first terminal device that is a sender of the packet data received by the reception unit; and

a memorizing unit operable to memorize a table indicating at least the address information acquired by the source acquisition unit as well as the types of secure protocols, encryption algorithms and encryption keys, judged by the judgment unit,

wherein the conversion unit acquires the address information from the source acquisition unit, and converts, with reference to the table, the secure protocol for the packet data sent

from the first terminal device on the external network into the secure protocol for the home network.

3. The packet routing device according to Claim 1,

wherein the packet data received by the reception unit contains a header part including plaintext communication control information and encrypted communication control information, and a main part including encrypted user information, and

the packet routing device further comprises:

an i dentification unit operable to identify the encrypted communication control information from the received packet data;

a decryption unit operable to decrypt the identified encrypted communication control information; and

a packet generation unit operable to generate packet data whose protocol is converted by the conversion unit, the packet data including the decrypted communication control information and the user information,

wherein the conversion unit converts the communication control information decrypted by the decryption unit into communication control information complying with the second secure protocol, and

the outputting unit outputs the packet data generated by the packet generation unit to the second secure protocol.

4. The packet routing device according to Claim 3,

wherein the judgment unit judges whether or not the first and the second terminal devices share a secure protocol, using the plaintext communication control information included in the header part, and

the conversion unit does not perform protocol conversion when the judgment unit judges that said first and second terminal devices share the secure protocol, but performs protocol

conversion only for the header part when it is judged that said first and second terminal devices do not share the secure protocol.

5. The packet routing device according to Claim 3,

wherein the judgment unit judges whether the first and the second terminal devices share a secure protocol, an encryption algorithm and an encryption key, using the plaintext communication control information included in the header part, and

when the judgment unit judges that said first and second terminal devices share the secure protocol, the encryption algorithm and the encryption key, the outputting unit outputs, to the second terminal device, the packet data received by the reception unit, without performing protocol conversion.

6. The packet routing device according to Claim 3, further comprising:

an encryption unit operable to encrypt the decrypted communication control information decrypted by the decryption unit using the encryption algorithm and the encryption key used for the secure protocol for the home network based on the judgment made by the judgment unit, after the decrypted communication control information is converted, as a plaintext, into communication control information complying with the second secure protocol

the packet generation unit generates packet data including the communication control information encrypted by the encryption unit and the user information.

7. The packet routing device according to Claim 6,

wherein the encryption algorithm for either of the following uses: for the decryption performed by the decryption unit and for

the encryption performed by the encryption unit, is one of the followings: Data Encryption Standard (DES), Triple DES (3DES) and Advanced Encryption Standard (AES).

8. The packet routing device according to Claim 3,

wherein the packet data received from the first terminal device further includes position information X indicating a storage position of the encrypted communication control information in the packet data, and

the identification unit identifies the encrypted communication control information based on the position information X.

9. The packet routing device according to Claim 3,

wherein the packet data received from the first terminal device further includes position information Y indicating a storage position of the user information in the packet data, and

the identification unit identifies the user information based on the position information Y.

10. The packet routing device according to Claim 3, further comprising a communication control information position registration unit operable to register, in the plaintext communication control information, information on head position and end position of the communication control information which has been protocol converted.

11. The packet routing device according to Claim 3, further comprising a user information position registration unit operable to register, in the plaintext communication control information, information on head position and end position of the encrypted user information.

12. The packet routing device according to Claim 3, further comprising an analysis unit operable to analyze whether or not an encryption block length of the communication control information is a multiple of a processing block used for encryption algorithm, and

wherein when the analysis unit analyzes that the encryption block length of the communication control information is a multiple of the processing block used for encryption algorithm, the decryption unit decrypts the analyzed communication control information, the conversion unit converts the decrypted communication control information into communication control information complying with the second secure protocol, the packet generation unit generates packet data including the converted communication control information and the user information, and then, the outputting unit outputs the generated packet data to the second terminal device, and

when the analysis unit analyzes that the encryption block length of the communication control information is not a multiple of the processing block used for encryption algorithm, the analysis unit sets a length of data to be decrypted so that said length of data becomes a multiple of the encryption algorithm, the decryption unit decrypts the communication control information and the user information, each of which is equivalent to the length of the data to be decrypted, the conversion unit converts the decrypted communication control information into communication control information complying with the second secure protocol and attaches padding data to the user information so that said user information becomes a multiple of the processing block used for encryption algorithm, the packet generation unit generates packet data including the converted communication control information and the user information, and then, the outputting unit outputs the generated packet data to the second terminal device.

13. The packet routing device according to Claim 3,

wherein the judgment unit judges whether or not the first and the second terminal devices share an encryption algorithm and an encryption key, using the plaintext communication control information included in the packet data received from the first terminal device, and

when the judgment unit judges that said first and second terminal devices share the encryption algorithm and the encryption key, the identification unit identifies the encrypted communication control information from the packet data, the decryption unit decrypts the identified communication control information, the conversion unit converts the decrypted communication control information into communication control information complying with the second secure protocol, the packet generation unit generates packet data including the converted communication control information and the user information, and then, the outputting unit outputs the generated packet data to the second terminal device, and

when the judgment unit judges that said first and second terminal devices do not share the encryption algorithm and the encryption key, the decryption unit decrypts both the communication control information and the user information, the conversion unit converts the decrypted communication control information into communication control information complying with the second secure protocol, the packet generation unit generates packet data including the converted communication control information and the user information, and then, the outputting unit outputs the generated packet data to the second terminal device.

14. The packet routing device according to Claim 13,

wherein the packet data received from the first terminal

device further includes identifying information which identifies the encryption algorithm and the encryption key used for the secure protocol for the packet data, and

the judgment unit judges whether or not said secure protocol and the second secure protocol share the encryption algorithm and the encryption key based on the identifying information.

15. The packet routing device according to Claim 3,

wherein the packet data received from the first terminal device includes an initial vector for decrypting head data of the encrypted communication control information in the packet data, and

the decryption unit decrypts the encrypted communication control information based on the initial vector.

16. The packet routing device according to Claim15, further comprising the following units when the decryption unit and the encryption unit require encrypted information having a data length of the processing block used for encryption algorithm and preceding the encrypted/decrypted communication control information by one block, for decrypting and encrypting said information:

an initial vector storage unit operable to store, in the plaintext communication control information, the encrypted communication control information as an initial vector necessary for decrypting head data of the user information, before the encrypted communication control information is decrypted, said encrypted communication control information preceding the user information by one block; and

an initial vector registration unit operable to register the initial vector stored in the initial vector storage unit in the plaintext

communication control information converted, as a plaintext, in compliance with the second secure protocol.

17. The packet routing device according to Claim 15,

wherein the packet data further includes a chain encryption flag indicating whether or not to chain decrypt the encrypted communication information and the encrypted user information, and

the decryption unit decrypts the encrypted user information based on the chain encryption flag.

18. The packet routing device according to Claim 15,

wherein encryption algorithm for either of the following uses: for the decryption performed by the decryption unit and the encryption performed by the encryption unit, is one of the followings: DES-Cipher Block Chaining (CBC), 3DES-CBC and AES-CBC.

19. The packet routing device according to Claim 3, further comprising a storage position registration unit operable to modify storage position information of the encrypted communication control information to storage position information of the decrypted communication control information, and register the modified storage position information in a predetermined position within the packet data.

20. The packet routing device according to Claim 3, further comprising a second storage position registration unit operable to modify storage position information of the encrypted user information to storage position information of the decrypted user information, and register the modified storage position information in a predetermined position within the packet data.

21. The packet routing device according to Claim 3,

wherein the packet routing device is connected to a plurality of terminal devices,

the conversion unit converts the decrypted communication control information to communication control information complying with a secure protocol for a destination terminal device connected to the packet routing device,

the packet generation unit generates packet data including the converted communication control information and the user information, and

the outputting unit outputs the generated packet data to the destination terminal device.

22. The packet routing device according to Claim 1,

wherein the packet data received from the first terminal device further includes identifying information which identifies the secure protocol, the encryption algorithm and the encryption key, used for the secure protocol for the packet data, and

the judgment unit judges whether or not the external network and the home network share the secure protocol, the encryption algorithm and the encryption key, based on the identifying information.

23. The packet routing device according to Claim 1, further comprising a destination identification unit operable to identify the first terminal device which is a destination of the packet data to be transmitted from the second terminal device on the home network,

wherein the conversion unit converts the secure protocol for the packet data into the secure protocol for the first terminal device on the external network, identified by the destination identification unit, and

the outputting unit outputs the packet data whose protocol

is converted by the conversion unit to the first terminal device that is the destination in the external network.

24. The packet routing device according to Claim 23,

wherein the conversion unit performs protocol conversion only for a header part of the packet data when the judgment unit judges that the second terminal device on the home network and the first terminal device on the external network do not share the secure protocol, but does not perform protocol conversion for the packet data when the judgment unit judges that the second terminal device on the home network and the first terminal device on the external network share the secure protocol.

25. A packet routing system for transmitting packet data via a packet routing device between a first terminal device on an external network and a second terminal device on a home network, the packet routing system comprising:

a reception unit operable to receive, from the first terminal device via the external network, the packet data complying with one of a plurality of secure protocols;

a judgment unit operable to judge types of secure protocols, encryption algorithms and encryption keys, used for communications via the external network and communications via the home network;

a conversion unit operable to convert a secure protocol for the packet data received by the reception unit into a second secure protocol for the home network, based on the judgment made by the judgment unit; and

an outputting unit operable to output, to the second terminal device, the packet data whose protocol has been converted by the conversion unit.

26. A packet routing method of routing packet data between a first terminal device on an external network and a second terminal device on a home network, the packet routing method comprising:

a reception step of receiving, from the first terminal device via the external network, the packet data complying with one of a plurality of secure protocols,;

a judgment step of judging types of secure protocols, encryption algorithms and encryption keys, used for communications via the external device and communications via the home network;

a conversion step of converting a secure protocol for the packet data received in the reception step into a second secure protocol for the home network; and

an outputting step of outputting, to the second terminal device, the packet data whose protocol has been converted in the conversion step.

27. The packet routing method according to Claim 26,

wherein the packet data received in the reception step contains a header part including plaintext communication control information and encrypted communication control information, and a main part including encrypted user information, and

the packet routing device further comprises:

an identification step of identifying the encrypted communication information from the received packet data;

a decryption step of decrypting the identified encrypted communication control information;

a packet generation step of generating packet data including the communication control information whose protocol is converted in the conversion step and the user information,

wherein in the conversion step, the communication control information decrypted in the decryption step is converted into

communication control information complying with the second secure protocol, and

in the outputting step, the packet data generated in the packet generation step is outputted to the second terminal device.

28. A program for a packet routing device which outputs packet data received from a first terminal via an external network complying with one of a plurality of secure protocols to a second terminal device via a home network complying with a second secure protocol, the program causing a computer to execute all the units included in the packet routing device according to any one of Claims 1 through 24.